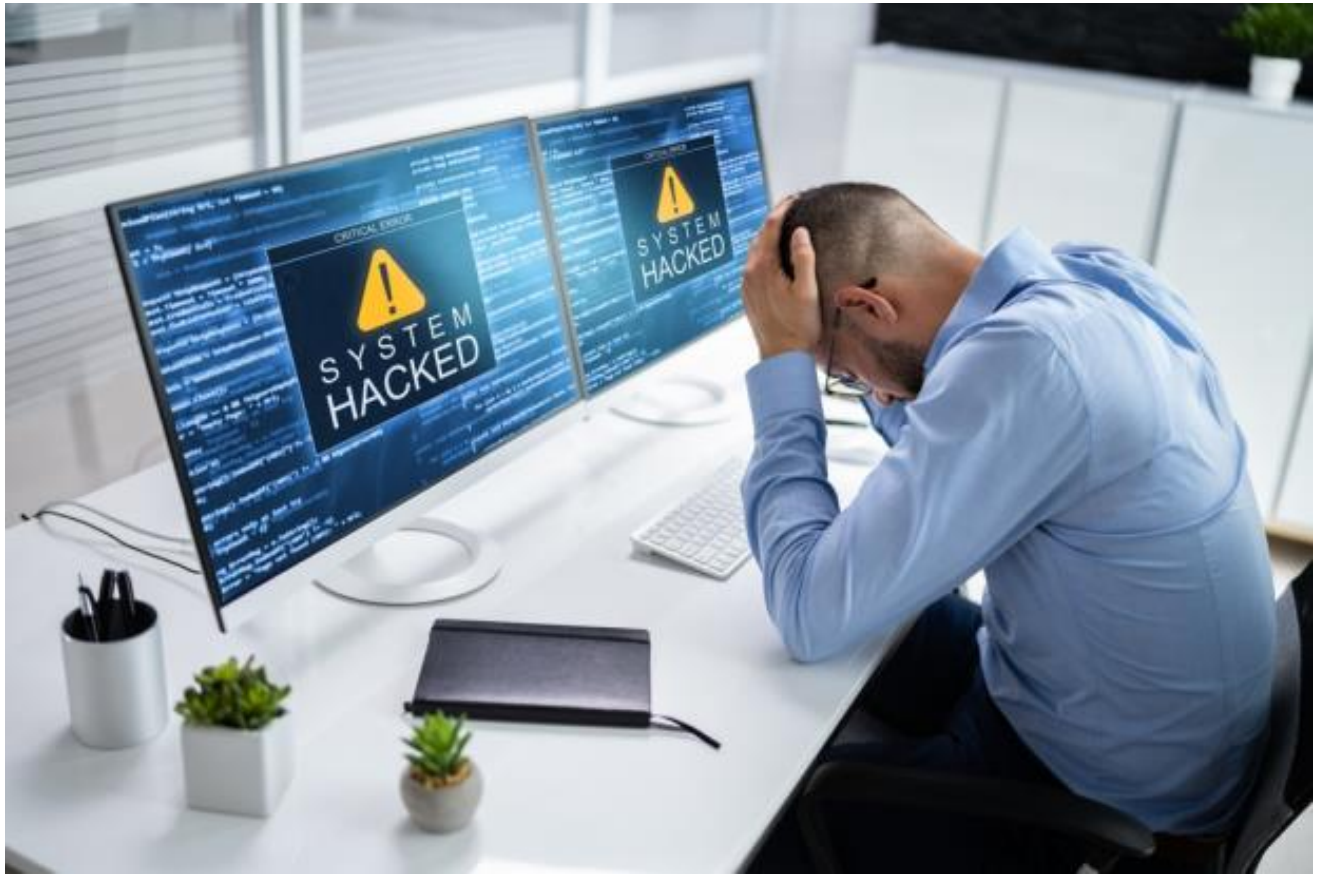
APZD - kybernetická bezpečnosť

Ing. Tomáš Antonič

biznis.slovanet.net

PRIEBEH ÚTOKU



MÄSPOMA – prípadová štúdia

V roku **2022** bol na spoločnosť **Mäspoma** prevedený **ransomwarový útok**, výsledkom ktorého boli zašifrované dáta

Hacker **zablokoval** takmer **všetky IT systémy** od účtovníctva, cez spracovanie objednávok až po emailovú komunikáciu.

Od firmy požadoval **výkupné pol milióna eur**.

Boli sme zavolaní na **vyriešenie** problému.
(samozrejme nie formou úhrady výkupného)

MÄSPOMA – prípadová štúdia

Celkovo viac ako **100 hodín čistého času** práce celého tímu našich ľudí (špecialisti na sieťovú bezpečnosť, špecialisti na inštaláciu, konfiguráciu a správu serverov a sieťových prvkov, špecialisti na Microsoft cloud produkty)

Prestávku mali len na spánok. Trvalo im to spolu viac ako **2 týždne**. Okrem našich ľudí samozrejme participovalo aj IT oddelenie klienta. (náklady na interných zamestnancov)

Infraštruktúru bolo potrebné vybudovať nanovo od nuly, čo zahŕňa inštaláciu virtualizačného prostredia, nanovo inštaláciu servera s Active Directory doménou, SQL servera, obnovenie databáz zo záloh atď.

MÄSPOMA – prípadová štúdia

V spomenutých hodinách čistého času nie sú zahrnuté procesy, ktoré bežali automaticky, ale samozrejme **predlžovali celkový čas** od vzniku incidentu, až po nábeh systémov.

Tento čas je len časom potrebným pre **nábeh základných systémov**, ktoré boli nevyhnutné na fungovanie firmy.

Postupne nasledovali ďalšie kroky spojené so zvýšením bezpečnosti, nasadenie FortiToken-ov, doladenie konfigurácie a pravidiel bezpečnosti. To bol **ďalší týždeň** prác, ktoré už ale mohli prebiehať postupne za chodu spoločnosti.

ČO POTREBUJETE

Čo **potrebujete** bez ohľadu na zákony **už dnes** a veľmi pravdepodobne bude vyžadované formou zákona a vyhlášky podľa NIS2?

- veľmi **rozsiahla téma**, ktorú je potrebné mať naštudovanú, alebo mať vhodných partnerov, ktorí vám pomôžu

- nasledujúce podtémy **nie sú** zďaleka **všetky**, predstavujú len malú časť toho, čo aj vaša spoločnosť potrebuje

ČO POTREBUJETE

Ochrana endpointov

Antivírus nestačí!

Anti-phishing
Šifrovanie disku
Dvojfaktorová autentifikácia
EDR/XDR systém
Ochrana pred sieťovými útokmi (lokálny firewall)

ČO POTREBUJETE

Segmentácia siete

Otázkou nie je **či** segmentovať, ale ako **správne segmentovať**

Ransomvérový útok nie je izolovaný len na jedno zariadenie.
Jeho **podstatou je rozšíriť sa** ďalej do siete a získať
a následne zašifrovať (prípadne poškodiť) čo najviac dát.
Dobrá segmentácia siete môže útočníka "**vymknúť**" len
v určitom segmente a nešíriť sa ďalej.

Nezabúdajte aj na vytvorenie **segmentov pre dodávateľov**, ktorí
z nejakého dôvodu musia pristupovať do vašej infraštruktúry na diaľku.

ČO POTREBUJETE

Pravidlá minimálnych privilégií

Používajte **princípy najnižších privilégií a architektúry nulovej dôvery** (least privilege principle, zero trust architecture), ktoré zabezpečia, že sa každý dostane len k údajom a aplikáciám, ktoré nevyhnutne potrebuje.

Ako to overiť? Monitoring, logovanie, kontrola.

ČO POTREBUJETE

Pravidelné školenia

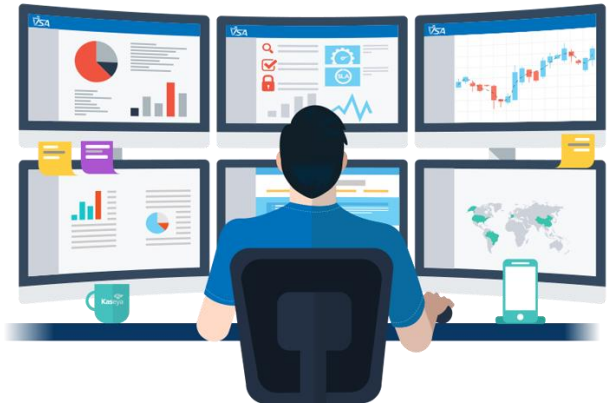
Vzdelávajte zamestnancov a budujte bezpečnostné povedomie v spoločnosti.
Chráňte vašu spoločnosť pred hrozbami a nástrahami kybernetického priestoru
Minimalizujte šance útočníkov uspieť pri útoku
Zvyšujte schopnosť vašej spoločnosti **odolávať** kybernetickým hrozbám

Školenia pre zamestnancov je možné poskytovať on-site ale aj vzdialene on-line formou e-learningu.

AKO RIEŠITE KYBERNETICKÉ INCIDENTY?

Aké sú predpoklady

Monitoring – prostredie a systémy musíte vedieť monitorovať
Detekcia – musíte byť schopný incident zdetegovať
Analýza – zdetegovaný incident musíte vedieť zanalyzovať
Reporting – zanalyzovaný incident musíte vedieť odreportovať



slovanet

Ako vám môžme pomôcť?

biznis.slovanet.net

Prezentujúci

Tomáš Antonič

Cyber Security Specialist

+421 903 374 675

tomas.antonic@slovanet.net

Obchodný kontakt

Tomáš Rak

Head of KAM

+421 918 885 555

tomas.rak@slovanet.net

Informácie

www.nis2info.sk

biznis.slovanet.net